[Claims]

(1) A system for performing user authentication for a computing environment including a plurality of servers among which relationships of mutual trust have been established, the system comprising:

an authentication policy table for registering authentication policies of at least one of the plurality of servers;

means for receiving authentication information from a user;

means for identifying, from among the plurality of servers, at least one server that adopts an authentication policy to which the authentication information matches with the use of the authentication policy table;

means for sending a signal to direct an authentication mechanism of the server identified by the means for identifying a server to perform user authentication with the use of the authentication information; and

means for permitting the user to access the computing environment on condition of success of the user authentication.

(2) The system according to Claim 1, further comprising:

means for obtaining information on the authentication policies of at least one of the plurality of servers; and

means for registering the obtained authentication policies of at least one of the plurality of servers in the authentication policy table while relating to the authentication policies to identifiers for identification of the servers adopting the authentication policies.

(3) The system according to Claim 1, further comprising:

means for identifying two or more servers adopting authentication policies identical to each other with the use of the authentication policy table;

means for determining whether or not user IDs identical to each other are respectively registered in the authentication systems of the two or more servers identified as ones adopting authentication policies identical to each other by the means for identifying a server;

means for receiving information for determination as to whether or not the user IDs identical to each other belong to one user on condition that the user IDs identical to each other are registered; and

means for registering the same user ID in an exception processing table on condition that the user IDs identical to each other do not belong to the one user.

(4) The system according to Claim 1, further comprising:

means for receiving authentication information from a new user;

means for identifying a server adopting the same authentication policy as an authentication policy indicated by the authentication information from the new user with the use of the authentication policy table;

means for determining whether or not the same user ID as a user ID indicated by the authentication information from the new user is registered in the authentication system of the identified server;

means for receiving information for determination as to whether or not the user IDs belong to the one user on condition that the same user ID is registered; and

means for registering the same user ID in an exception processing table on condition that the user IDs do not belong to the one user.

(5) The system according to Claim 1, wherein the authentication policy is at least one of authentication using a character-string user ID, authentication using a client certificate, biometrics, and handwriting authentication.

(6) The system according to Claim 1, wherein the means for permitting access includes means for generating a token for access to the computing environment.

(7) The system according to Claim 6, wherein the token is one of a cookie, authentication information based on URL encoding and an SAML token.

(8) The system according to Claim 1, comprising a plurality of authentication policy tables with respect to a plurality of computing environments, wherein user authentication is

performed with respect to each of the plurality of computing environments in response to matching of authentication information received from a user with servers registered in the plurality of authentication policy table.

(9) A method in a computing environment including a plurality of servers among which relationships of mutual trust have been established, at least one of the plurality of servers holding an authentication policy table for registering authentication policies of at least one of the plurality of servers, the method comprising the steps of:

receiving authentication information from a user;

identifying, from among the plurality of servers, at least one server that adopts an authentication policy to which the authentication information matches with the use of the authentication policy table;

sending a signal to direct an authentication mechanism of the server identified in the step of identifying a server to perform user authentication with the use of the authentication information; and

permitting the user to access the computing environment on condition of success of the user authentication.

(10) The method according to Claim 9, further comprising the steps of:

obtaining information on the authentication policies of at least one of the plurality of servers; and

registering the obtained authentication policies of at least one of the plurality of servers in the authentication policy table while relating to the authentication policies to identifiers for identification of the servers adopting the authentication policies.

(11) The method according to Claim 9, further comprising the steps of:

identifying two or more servers adopting authentication policies identical to each other with the use of the authentication policy table;

determining whether or not user IDs identical to each other

are respectively registered in the authentication systems of the two or more servers identified as ones adopting authentication policies identical to each other in the step of identifying a server;

receiving information for determination as to whether or not the user IDs identical to each other belong to one user on condition that the user IDs identical to each other are registered; and

registering the same user ID in an exception processing table on condition that the user IDs identical to each other do not belong to the one user.

(12) The method according to Claim 9, further comprising the steps of:

receiving authentication information from a new user;

identifying a server adopting the same authentication policy as an authentication policy indicated by the authentication information from the new user with the use of the authentication policy table;

determining whether or not the same user ID as a user ID indicated by the authentication information from the new user is registered in the authentication system of the identified server;

receiving information for determination as to whether or not the user IDs belong to the one user on condition that the same user ID is registered; and

registering the same user ID in an exception processing table on condition that the user IDs do not belong to the one user.

(13) The method according to Claim 9, wherein the authentication policy is at least one of authentication using a character-string user ID, authentication using a client certificate, biometrics, and handwriting authentication.

(14) The method according to Claim 9, wherein the step of permitting access includes a step of generating a token for access to the computing environment.

(15) The method according to Claim 14, wherein the token is one of a cookie, authentication information based on URL encoding and an SAML token.

(16) The method according to Claim 9, comprising the steps of:

(A) prioritizing two or more servers adopting authentication policies identical to each other and registered in the authentication policy table;

(B) directing the authentication mechanism of the server having the highest priority in the two or more servers to perform user authentication in response to matching of the authentication information from the user with the authentication policy adopted in the two or more servers;

(C) directing the authentication mechanism of the server having the next highest priority among the two or more servers to perform user authentication in response to failure to complete the user authentication;

(D) repeating the step (C) until the user authentication results in success or the user authentication results in failure in all of the two or more servers; and

(E) permitting the user to access the computing environment on condition of success of the user authentication.

(17) A program in a computing environment including a plurality of servers among which relationships of mutual trust have been established, at least one of the plurality of servers holding at least one authentication policy table for registering authentication policies of at least one of the plurality of servers, the program causing a computer to execute the steps of:

receiving authentication information from a user;

identifying, from among the plurality of servers, at least one server that adopts an authentication policy to which for the authentication information matches with the use of the authentication policy table;

sending a signal to direct an authentication mechanism of the server identified in the step of identifying a server to perform user authentication with the use of the authentication information; and

permitting the user to access the computing environment on condition of success of the user authentication.

(18) The program according to Claim 17, causing the computer to further execute the steps of:

obtaining information on the authentication policies of at least one of the plurality of servers; and

registering the obtained authentication policies of at least one of the plurality of servers in the authentication policy table while relating to the authentication policies to identifiers for identification of the servers adopting the authentication policies.

(19) The user authentication program according to Claim 17, causing the computer to further execute the steps of:

identifying two or more servers adopting authentication policies identical to each other with the use of the authentication policy table;

determining whether or not user IDs identical to each other are respectively registered in the authentication systems of the two or more servers identified as ones adopting authentication policies identical to each other in the step of identifying a server;

receiving information for determination as to whether or not the user IDs identical to each other belong to one user on condition that the user IDs identical to each other are registered; and

registering the same user ID in an exception processing table on condition that the user IDs do not belong to the one user.

(20) The user authentication program according to Claim 17, causing the computer to further execute the steps of:

receiving authentication information from a new user;

identifying a server adopting the same authentication policy as an authentication policy indicated by the authentication information from the new user with the use of the authentication policy table;

determining whether or not the same user ID as a user ID indicated by the authentication information from the new user is registered in the authentication system of the identified server;

determining as to whether or not the user IDs belong to the

one user on condition that the same user ID is registered; and registering the same user ID in an exception processing table on condition that the user IDs do not belong to the one user.

(21) The user authentication program according to Claim 17, wherein the authentication policy is at least one of authentication using a character-string user ID, authentication using a client certificate, biometrics, and handwriting authentication.

(22) The user authentication program according to Claim 17, wherein the step of permitting access includes a step of generating a token for access to the computing environment.

(23) The user authentication program according to Claim 22, wherein the token is one of a cookie, authentication information based on URL encoding and an SAML token.

(24) A computer readable storage medium on which the user authentication program according to any one of Claims 17 to 23 is recorded.